NHS
Mersey and West Lancashire
Teaching Hospitals
NHS Trust

Ref. No:	2204
Date:	03/12/25
Subject:	DSPT-Relevant Current & Incoming Suppliers

REQUEST

1. A list of all external suppliers, contractors, or partner organisations who currently fall within the remit of the NHS Data Security & Protection Toolkit (DSPT) for your organisation.

This includes any supplier that handles patient data, accesses NHS systems, or provides digital, software, cloud, data-processing, or cyber-security services requiring DSPT compliance.

2. A list of any new, incoming, or planned suppliers (contracted or due to go live within the next 12 months) who will fall within the DSPT remit for the same reasons.

3. For each supplier identified in Q1 or Q2, please confirm (if recorded):

- Whether they are required to maintain a “Standards Met” DSPT submission

- The date you last checked or verified their DSPT status (or expected verification date for new suppliers)

4. Does your organisation maintain an internal register or log of DSPT-relevant suppliers (including planned or onboarding suppliers)?

- If yes, please provide the relevant extract.

- If no, please confirm that no such register exists.

RESPONSE

You asked for a list of all external suppliers, contractors, or partner organisations who fall within the remit of the NHS Data Security & Protection Toolkit (DSPT), including current and planned suppliers, their DSPT compliance status, and any internal registers maintained.

Exemption Applied

We are unable to provide the requested detailed supplier information under Section 31(1)(a) of the Freedom of Information Act 2000 (Prevention or Detection of Crime). Disclosure of this information would pose a significant cybersecurity risk by identifying specific suppliers and systems that handle sensitive patient data. Publishing these details could make MWL and its partners more vulnerable to targeted cyberattacks.

Why Disclosure Would Create Risk

The NHS and its suppliers have been subject to serious cyber incidents in recent years, including:

Ivanti Endpoint Manager Mobile Exploit (May 2025)

- What happened: University College London Hospitals (UCLH) and University Hospital Southampton NHS Foundation Trust were breached after attackers exploited a vulnerability in Ivanti Endpoint Manager Mobile, a third-party tool used to manage staff mobile devices.
- Impact: Staff data such as mobile numbers and IMEI codes were exposed. No patient data was confirmed as accessed, but the incident highlighted supply chain risks.

Synnovis Pathology Supplier Ransomware Attack (June 2024)

- What happened: Synnovis, a pathology provider serving King’s College Hospital and Guy’s and St Thomas’ NHS Foundation Trust, was hit by a ransomware attack by the Qilin group.
- Impact: Thousands of appointments and surgeries were cancelled, blood testing services were disrupted for months, and sensitive patient data was stolen and leaked online.

Advanced Computer Software Group Attack (August 2022)

- What happened: Advanced, a major NHS software supplier, suffered a ransomware attack due to missing multi-factor authentication (MFA) and poor patch management.
- Impact: NHS 111 services and electronic patient record systems were taken offline, forcing staff to revert to manual processes. Data of nearly 80,000 individuals was compromised.

Releasing a full supplier list and DSPT compliance status could provide attackers with a roadmap of potential targets, increasing the likelihood of similar incidents.

Assurance on DSPT Compliance

Although we cannot share the detailed supplier list, please be assured that:

- All suppliers handling patient data or accessing NHS systems must comply with the NHS Data Security and Protection Toolkit (DSPT) and maintain a “Standards Met” status.

- MWL enforces DSPT compliance through:
    - Pre-contract checks: Suppliers must demonstrate DSPT compliance before onboarding.
    - Contractual obligations: DSPT compliance is a mandatory requirement in all relevant contracts.
    - Ongoing monitoring: We maintain an internal register of DSPT-relevant suppliers and review compliance status regularly.
- Suppliers are also required to provide cybersecurity assurance, including evidence of penetration testing, incident response plans, and adherence to NHS security standards.
- Our DPST evidence submission is independently audited before submission.

These measures ensure that suppliers meet NHS requirements for protecting patient data and mitigating cyber risks.